Ch. 1 – Scaling IP Addresses
NAT/PAT and DHCP

Cabrillo College

CIS 83 (CCNA 4)

Fall 2006

Rick Graziani

Cabrillo College

Note to instructors

- If you have downloaded this presentation from the Cisco Networking Academy Community FTP Center, this may not be my latest version of this PowerPoint.
- For the latest PowerPoints for all my CCNA, CCNP, and Wireless classes, please go to my web site:

  http://www.cabrillo.edu/~rgraziani/

  - The username is *cisco* and the password is *perlman* for all of my materials.
- If you have any questions on any of my materials or the curriculum, please feel free to email me at graziani@cabrillo.edu (I really don't mind helping.) Also, if you run across any typos or errors in my presentations, please let me know.
- I will add "(Updated – *date*)" next to each presentation on my web site that has been updated since these have been uploaded to the FTP center.

Thanks! Rick

Private addressing

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

- 172.16.0.0 – 172.31.255.255: 172.16.0.0/12
  - Where does the /12 come from?

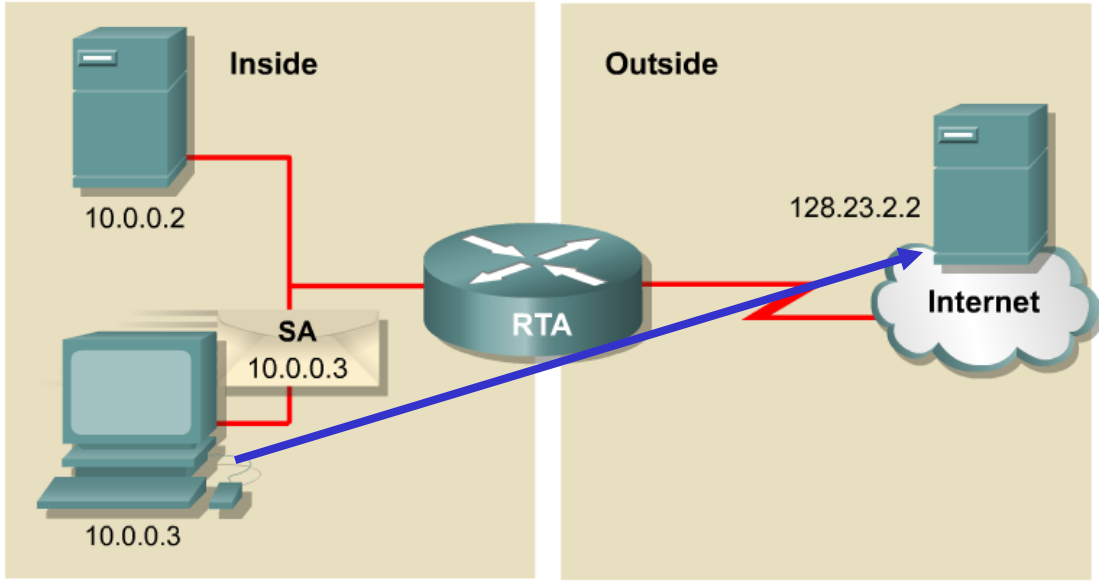
12 bits in common

10101100 . 00010000 . 00000000 . 00000000 – 172.16.0.0

10101100 . 00011111 . 11111111 . 11111111 – 172.31.255.255

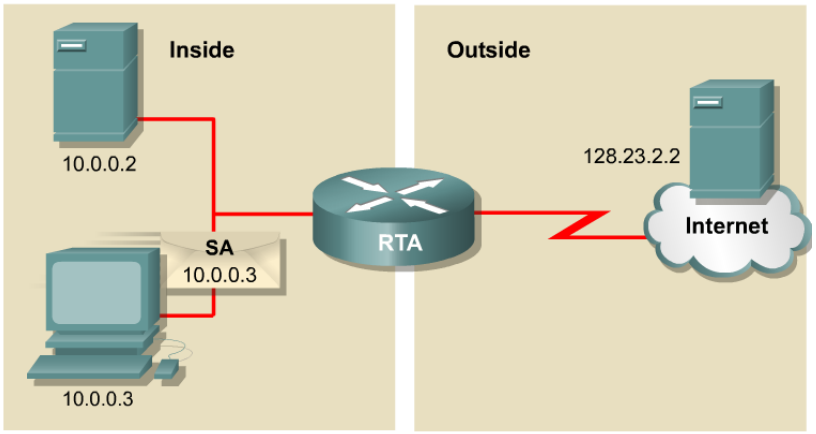
10101100 . 00010000 . 00000000 . 00000000 – 172.16.0.0/12

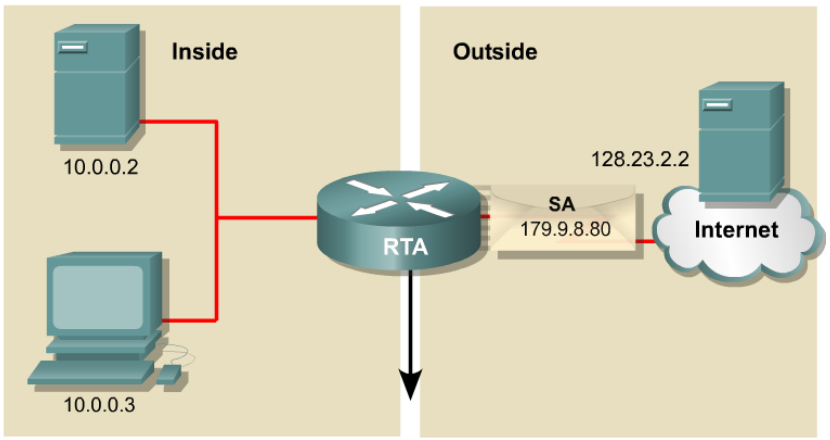
Introducing NAT and PAT



- NAT is designed to conserve IP addresses and enable networks to use private IP addresses on internal networks.
- These private, internal addresses are translated to routable, public addresses.
- **NAT**, as defined by RFC 1631, is the process of swapping one address for another in the IP packet header.
- In practice, NAT is used to allow hosts that are privately addressed to access the Internet.
- NAT translations can occur dynamically or statically.
- The most powerful feature of NAT routers is their capability to use **port address translation (PAT),** which allows multiple inside addresses to map to the same global address.
- This is sometimes called a many-to-one NAT.

NAT Example

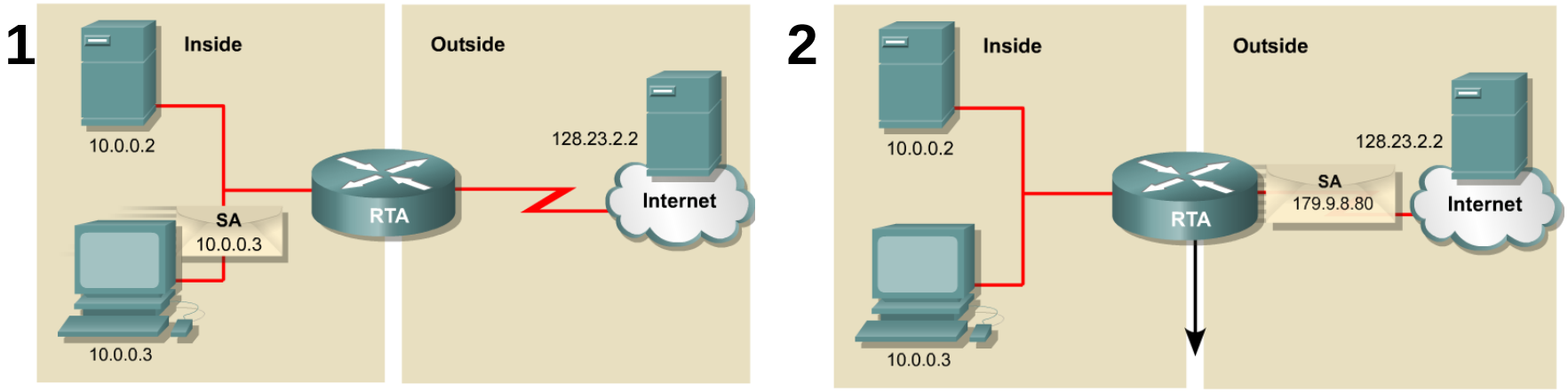




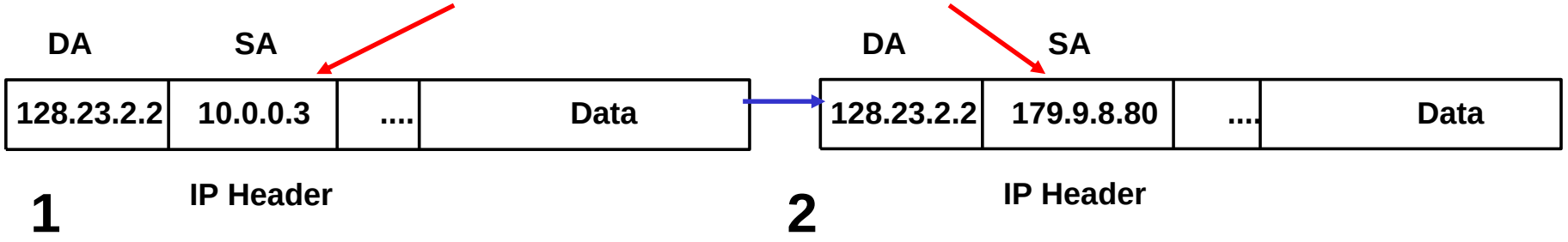
NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

- **Inside local address** – The IP address assigned to a host on the inside network. This address is likely to be an RFC 1918 private address.
- **Inside global address** – A legitimate (Internet routable or public) IP address assigned the service provider that represents one or more inside local IP addresses to the outside world.
- **Outside local address** – The IP address of an outside host as it is known to the hosts on the inside network.

NAT Example

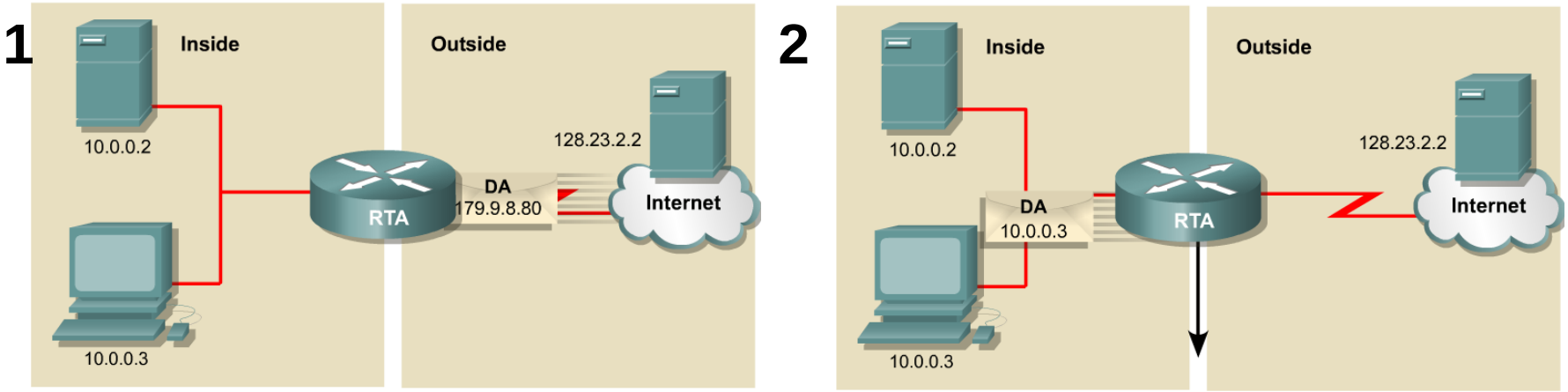


NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2



- The translation from Private source IP address to Public source IP address.

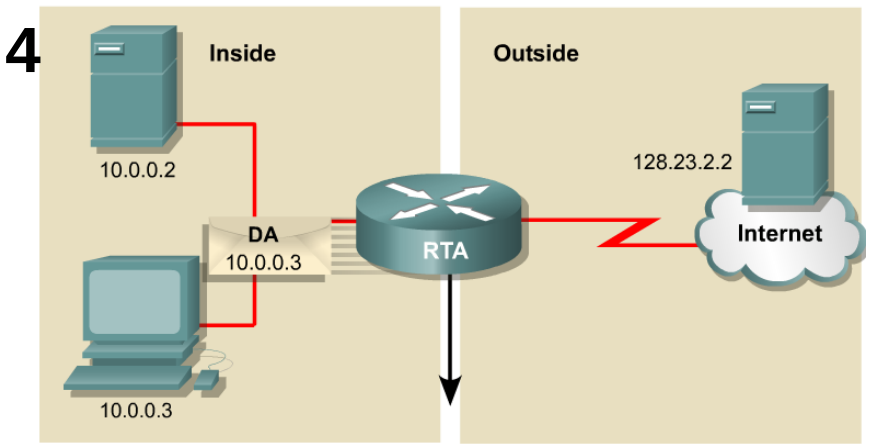
NAT Example

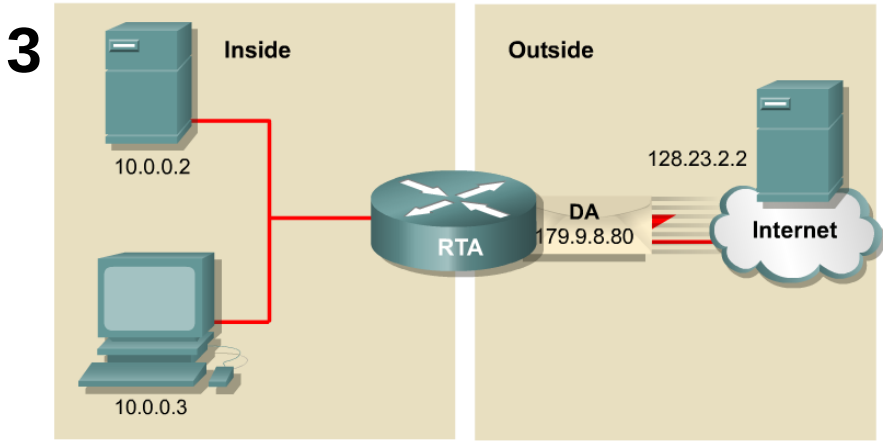


NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.2 10.0.0.3	179.9.8.80 179.9.8.80	128.23.2.2 128.23.2.2

- **Inside local address** – The IP address assigned to a host on the inside network.
- **Inside global address** – A legitimate (Internet routable or public) IP address assigned the service provider.
- **Outside global address** – The IP address assigned to a host on the outside network. The owner of the host assigns this address.

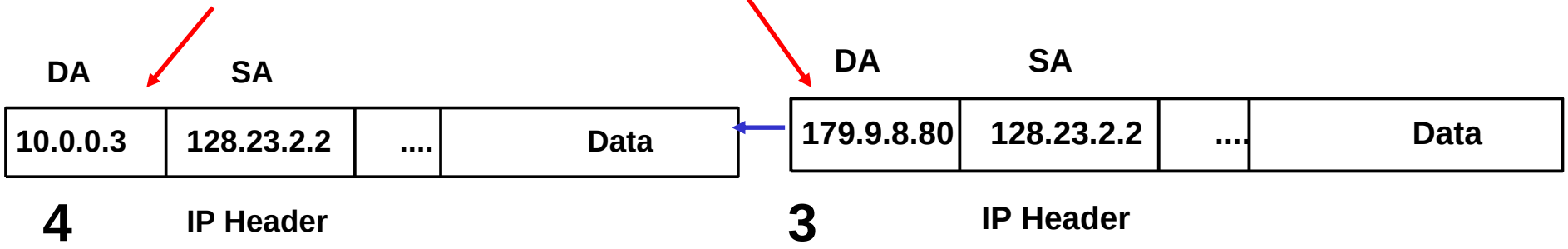
NAT Example





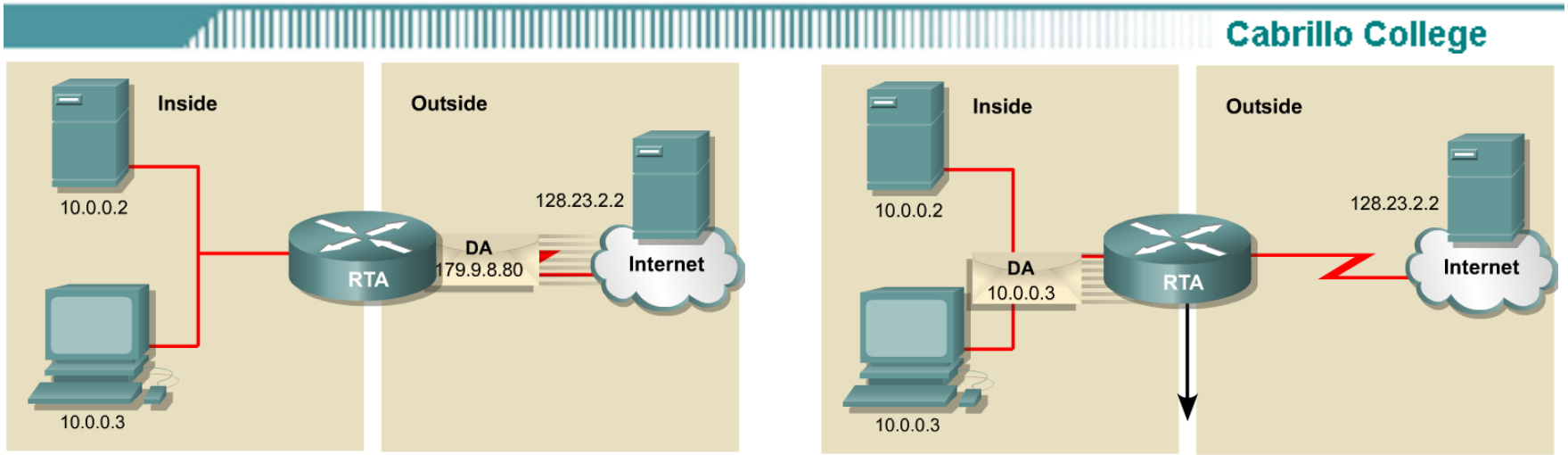
NAT Table

Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.2	179.9.8.80	128.23.2.2
10.0.0.3	179.9.8.80	128.23.2.2



- Translation back, from Public destination IP address to Private destination IP address.

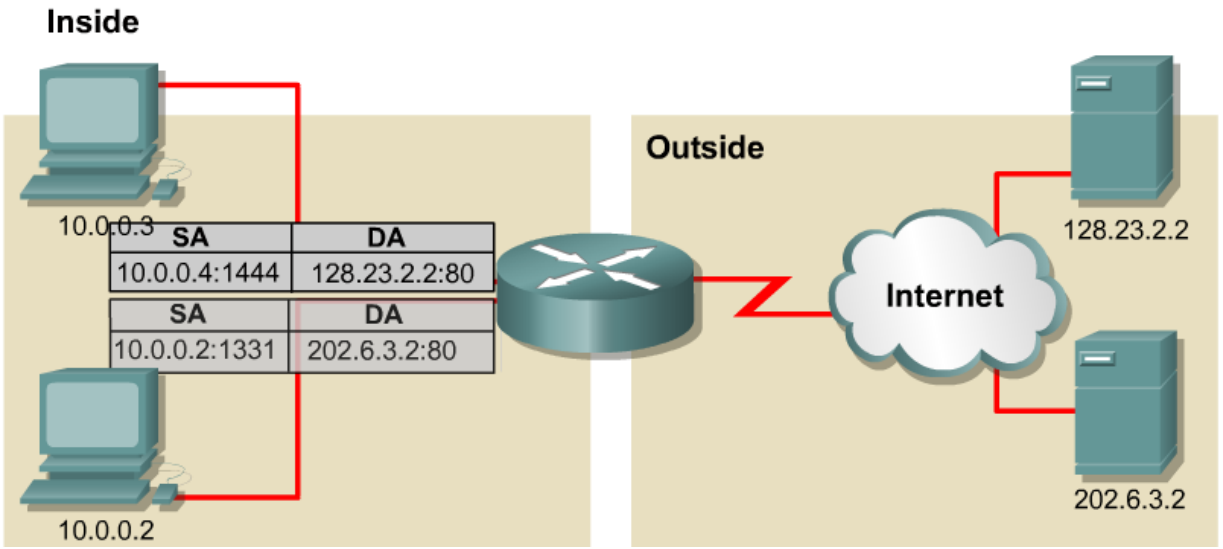
NAT Example



NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.2 10.0.0.3	179.9.8.80 179.9.8.80	128.23.2.2 128.23.2.2

- NAT allows you to have more than your allocated number of IP addresses by using RFC 1918 address space with smaller mask.
- However, because you have to use your Public IP addresses for the Internet, NAT still limits the number of hosts you can have access the Internet at any one time (depending upon the number of hosts in your public network mask.)

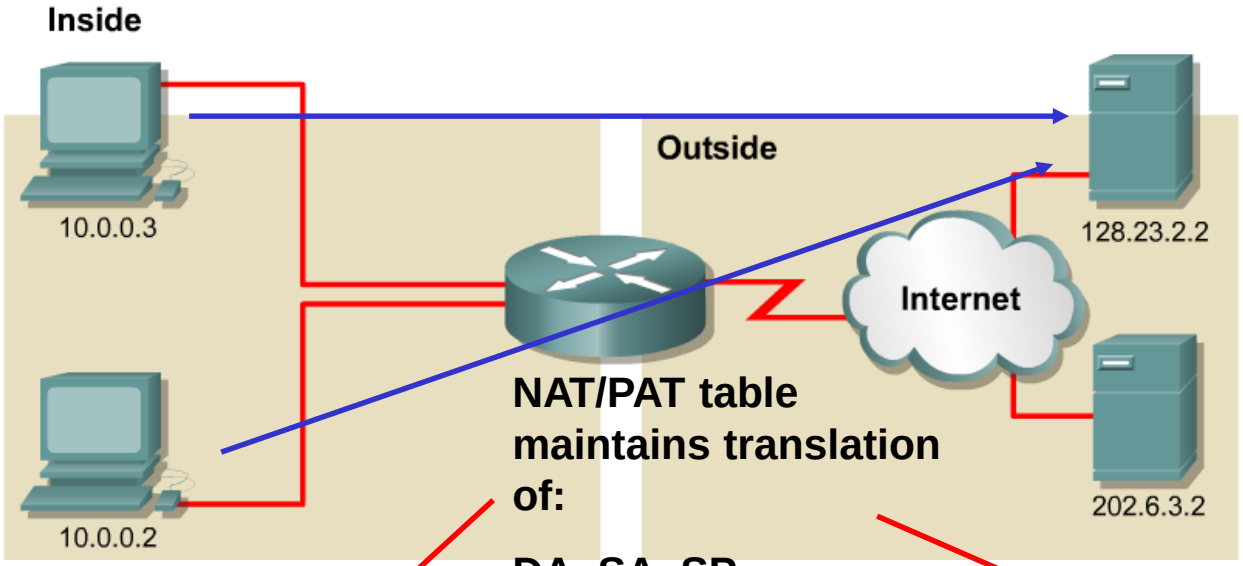
PAT – Port Address Translation



NAT Table			
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global Address
10.0.0.2:1331 10.0.0.3:1555	179.9.8.20:1331 179.9.8.20:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

- PAT (Port Address Translation) allows you to use a single Public IP address and assign it up to 65,536 inside hosts (4,000 is more realistic).
- PAT modifies the TCP/UDP source port to track inside Host addresses.
- Tracks and translates SA, DA and SP (which uniquely identifies each connection) for each stream of traffic.

PAT Example



DA	SA	DP	SP	
128.23.2.2	10.0.0.3	80	1331	Data

1

IP Header

TCP/UDP Header

DA	SA	DP	SP	
128.23.2.2	179.9.8.80	80	3333	Data

2

IP Header

TCP/UDP Header

DA	SA	DP	SP	
128.23.2.2	10.0.0.2	80	1555	Data

IP Header

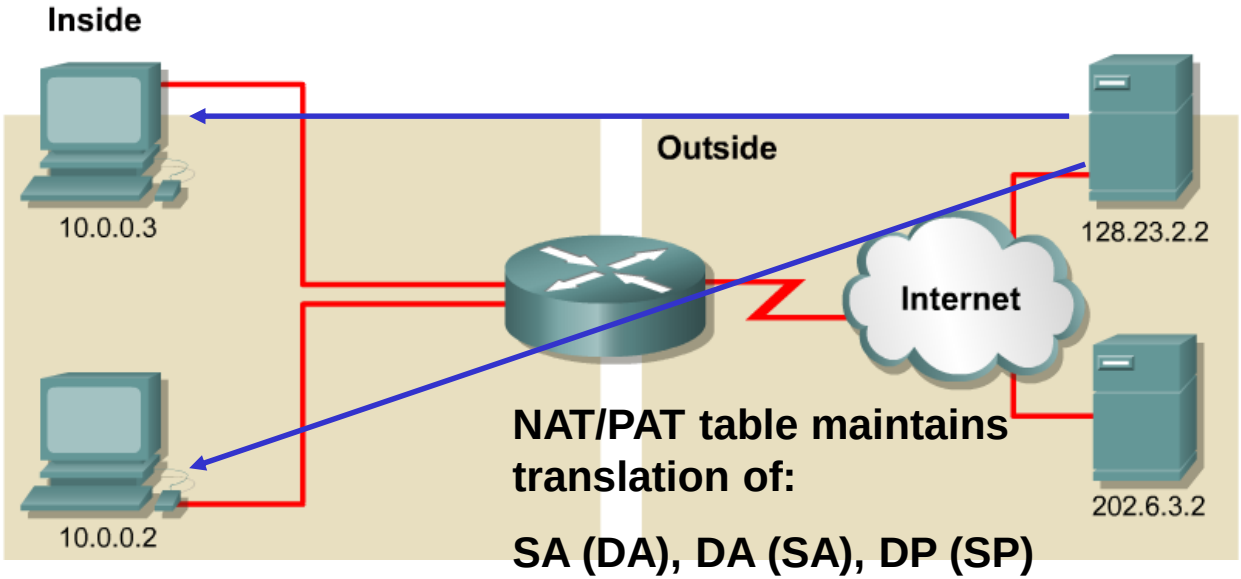
TCP/UDP Header

DA	SA	DP	SP	
128.23.2.2	179.9.8.80	80	2222	Data

IP Header

TCP/UDP Header

PAT Example



DA	SA	DP	SP	
10.0.0.3	128.23.2.2	1331	80	Data

IP Header | TCP/UDP Header

4

DA	SA	DP	SP	
179.9.8.80	128.23.2.2	3333	80	Data

IP Header | TCP/UDP Header

3

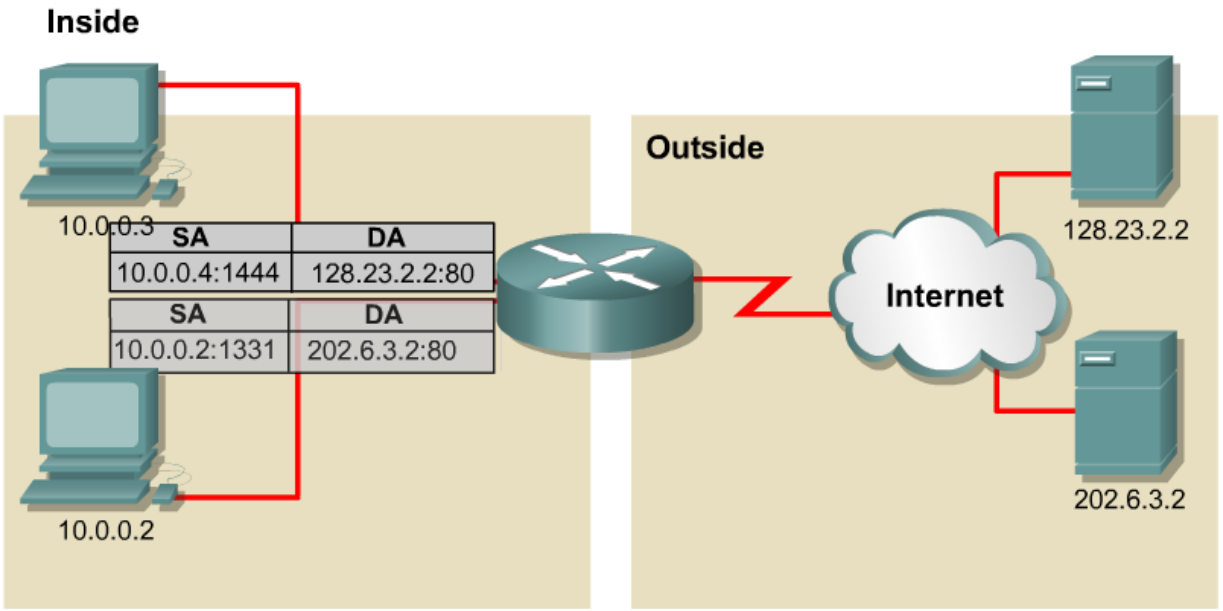
DA	SA	DP	SP	
10.0.0.2	128.23.2.2	1555	80	Data

IP Header | TCP/UDP Header

DA	SA	DP	SP	
179.9.8.80	128.23.2.2	2222	80	Data

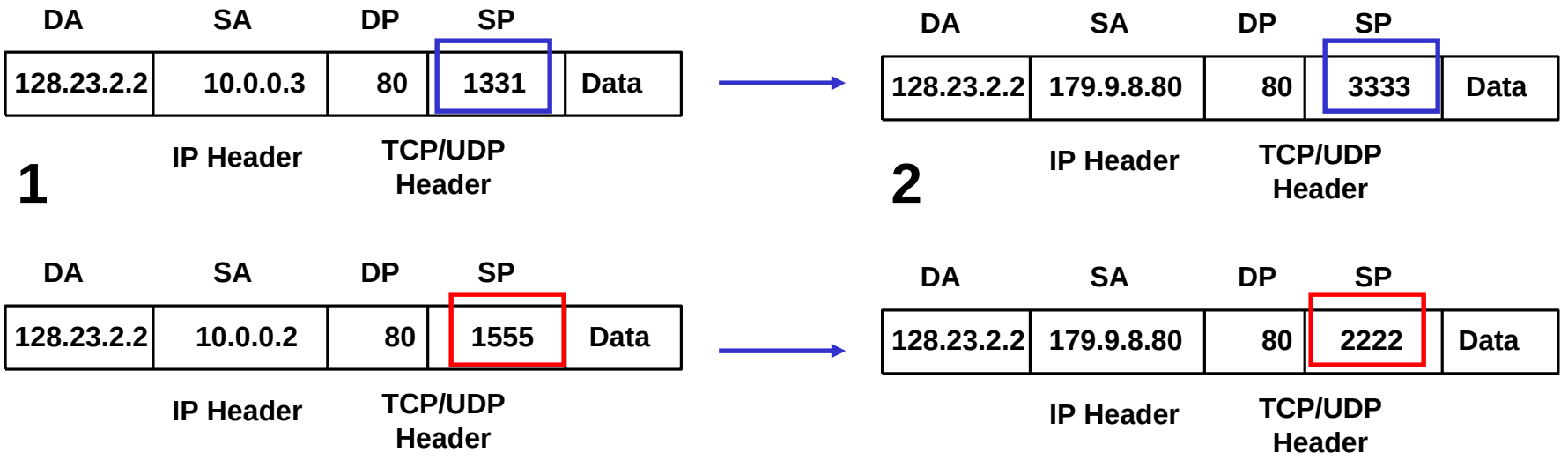
IP Header | TCP/UDP Header

PAT – Port Address Translation



- With PAT a multiple private IP addresses can be translated by a single public address (many-to-one translation).
- This solves the limitation of NAT which is one-to-one translation.

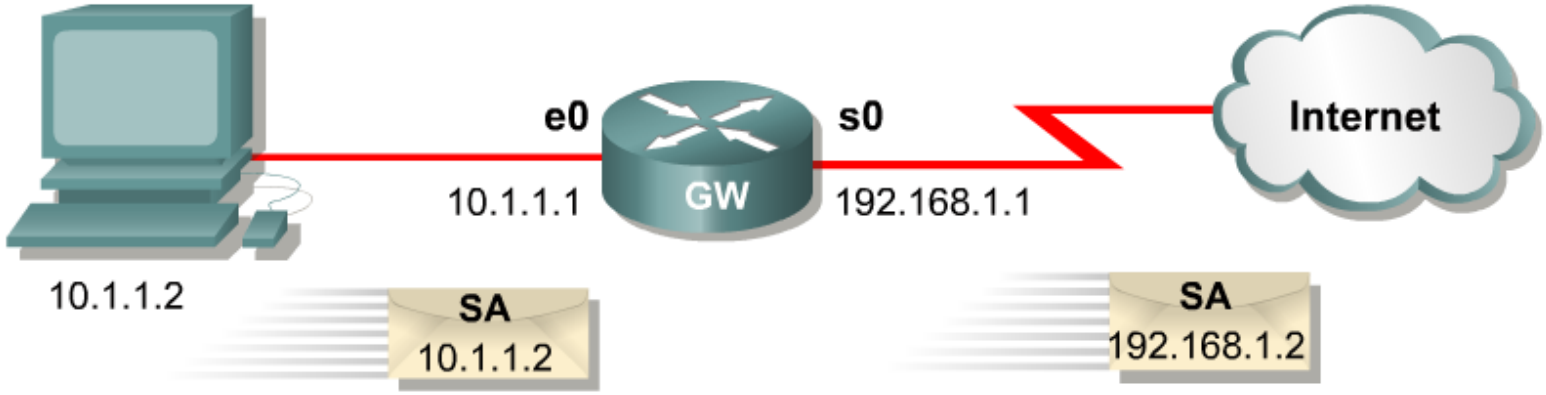
PAT – Port Address Translation



From CCNP 2 curriculum"

- "As long as the inside global port numbers are unique for each inside local host, NAT overload will work. For example, if the host at 10.1.1.5 and 10.1.1.6 both use TCP port 1234, the NAT router can create the extended table entries mapping 10.1.1.5:1234 to 171.70.2.2:1234 and 10.1.1.6:1234 to 171.70.2.2:1235. **In fact, NAT implementations do <u>not</u> necessarily try to preserve the original port number**."

Configuring Static NAT



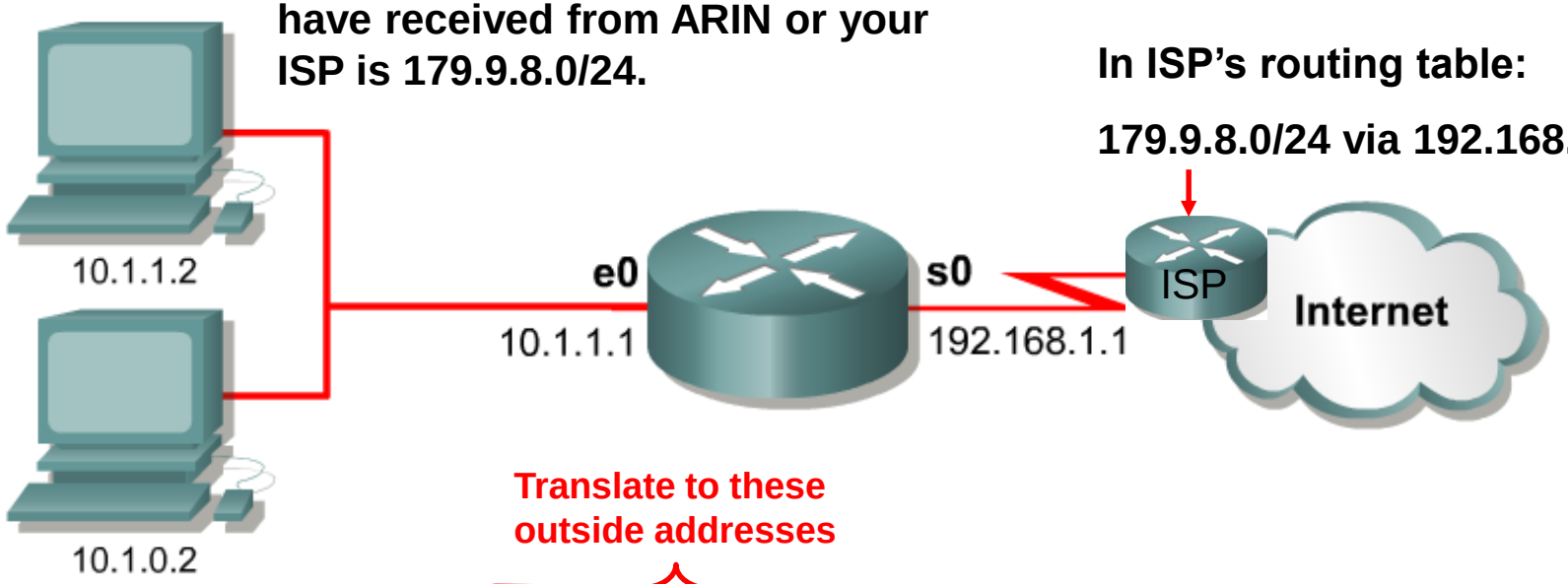

```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
```

Configuring Dynamic NAT

The network address space you have received from ARIN or your ISP is 179.9.8.0/24.

In ISP's routing table:

179.9.8.0/24 via 192.168.1.1



Translate to these outside addresses

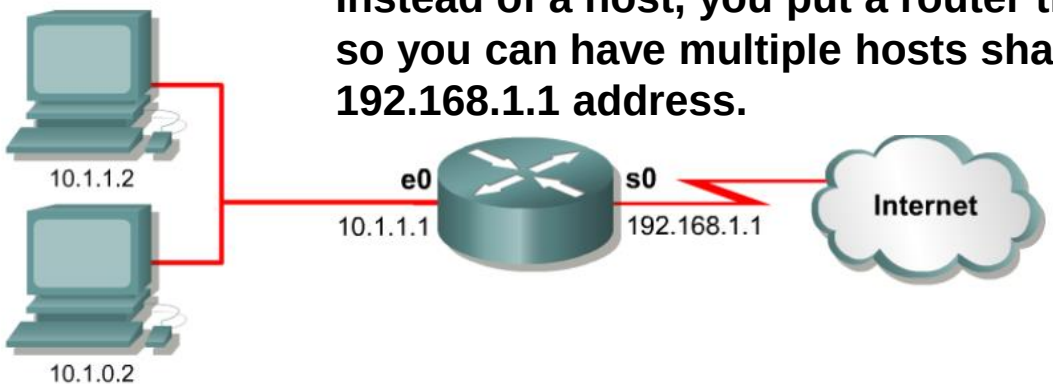
Start here

```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.255.255
```

Source IP address must match here

Configure PAT – Overload

192.168.1.1 is the address your ISP has assigned you. Instead of a host, you put a router there, running PAT so you can have multiple hosts share that same 192.168.1.1 address.

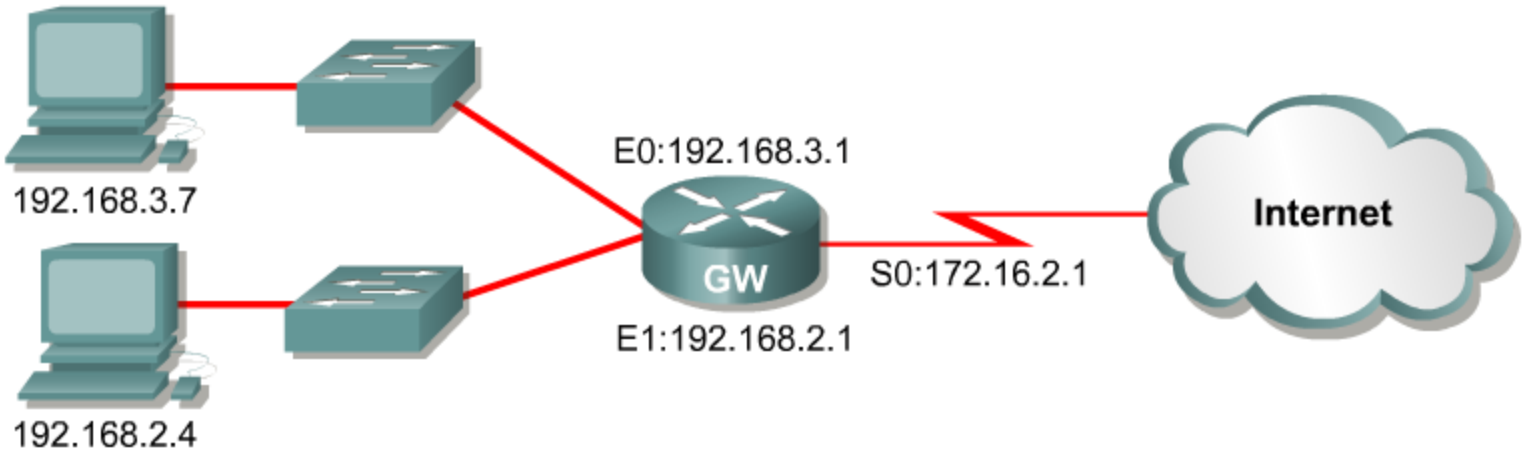



```
Router(config)#access-list 1 permit 10.1.0.0 0.0.255.255

Router(config)#ip nat pool nat-pool2 179.9.8.20 netmask
255.255.255.240

Router(config)#ip nat inside source list 1 pool nat-pool2
overload
```

- Establishes overload translation and specifies the IP address to be overloaded as that designated in the pool.

- In this example a single Public IP addresses is used, using PAT, source ports, to differentiate between connection streams.

Configure PAT – Overload




```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

This is a different example, using the IP address of the outside interface instead specifying an IP address

NAT/PAT Clear Commands


```
Router#clear ip nat translation
```

- Clears all dynamic address translation entries

```
Router#clear ip nat translation inside global-ip local-ip [outside
local-ip global-ip]
```

- Clears a simple dynamic translation entry

```
Router#clear ip nat translation protocol inside global-ip global-port
local-ip local-port [outside local-ip local-port global-ip
global-port]
```

- Clears an extended dynamic translation entry

Command	Description
clear ip nat translation *	Clears all dynamic address translation entries from the NAT translation table
clear ip nat translation inside *global-ip local-ip* **[outside** *local-ip global-ip*]	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation
clear ip nat translation protocol inside *global-ip global-port local-ip local-port* **[outside** *local-ip local-port global-ip global-port*]	Clears a simple dynamic translation entry

Verifying NAT/PAT


```
Router#show ip nat translations [verbose]
```

- Displays active translation

```
Router#show ip nat translation
Pro Inside global     Inside local       Outside local      Outside global
172.16.131.1          10.10.10.1               ---                ---
```

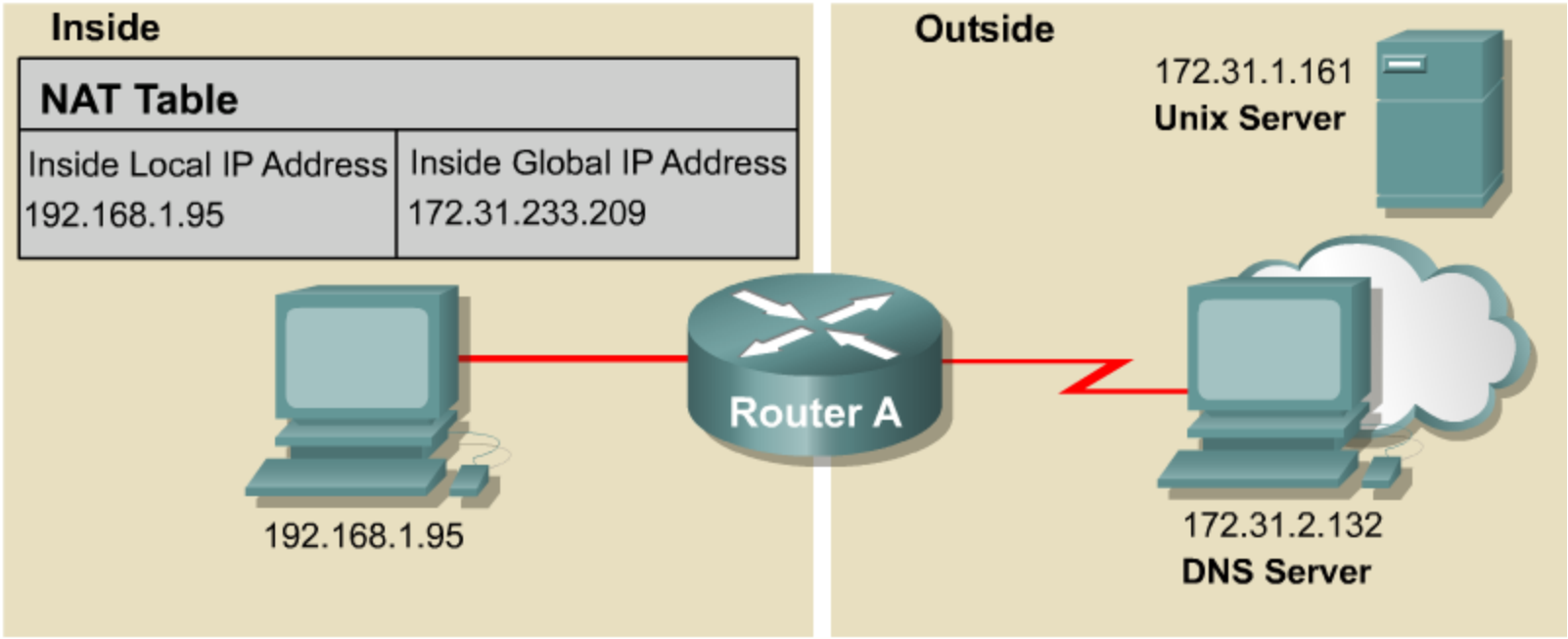
```
Router#show ip nat statistics
```

- Displays translation statistics

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0
```

Command	Description
`show ip nat translations`	Displays active translations
`show ip nat statistics`	Displays translation statistics

Troubleshooting NAT/PAT




```
RouterA#debug ip nat
NAT:   s= 192.168.1.95    → 172.31.233.209,          d=172.31.2.132 [6825]
NAT:   s= 172.31.2.132,     d=172.31.233.209,     → 192.168.1.95 [21852]
NAT:   s= 192.168.1.95    → 172.31.233.209,          d=172.31.1.161 [6826]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,     → 192.168.1.95 [23311]
NAT*:  s= 192.168.1.95    → 172.31.233.209,          d=172.31.1.161 [6827]
NAT*:  s= 192.168.1.95    → 172.31.233.209,          d=172.31.1.161 [6828]
NAT*:  s= 172.31.1.161      d=172.31.233.209,     → 192.168.1.95 [23313]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,     → 192.168.1.95 [23313]
```

Issues with NAT/PAT

NAT has several advantages, including the following:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets.
- NAT allows the existing scheme to remain, and it still supports the new assigned addressing scheme outside the private network.

- NAT also forces some applications that use IP addressing to stop functioning because it hides end-to-end IP addresses.
- Applications that use physical addresses instead of a qualified domain name will not reach destinations that are translated across the NAT router.
- Sometimes, this problem can be avoided by implementing static NAT mappings.

Cisco IOS NAT does support the following traffic types although they carry IP addresses in the application data stream:

- ICMP
- File Transfer Protocol (FTP), including PORT and PASV commands
- NetBIOS over TCP/IP, datagram, name, and session services
- Progressive Networks' RealAudio
- White Pines' CuSeeMe
- DNS "A" and "PTR" queries
- H.323/NetMeeting, versions 12.0(1)/12.0(1)T and later
- VDOLive, version 11.3(4)11.3(4)T and later
- Vxtreme, versions 11.3(4)11.3(4)T and later
- IP multicast, version 12.0(1)T, the source address translation only

Cisco IOS NAT does not support the following traffic types:

- Routing table updates
- DNS zone transfers
- BOOTP
- talk, ntalk
- Simple Network Management Protocol (SNMP)

DHCP
Dynamic Host Configuration Protocol

The first several slides should be a review of DHCP from CCNA 1.

We will start with the discussion of configuring DHCP on a Cisco router.

Please read the online curriculum if you need a review.

Introducing DHCP

Ethernet Frame	IP	UDP	DHCP Request
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	IP SRC: ? IP DST: 255.255.255.255	UDP 67	CIADDR: ? GIADDR: ? Mask:? CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

Ethernet Frame	IP	UDP	DHCP Reply
SRC MAC: MAC Serv DST MAC: MAC A	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 GIADDR: ? Mask: 255.255.255.0 CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

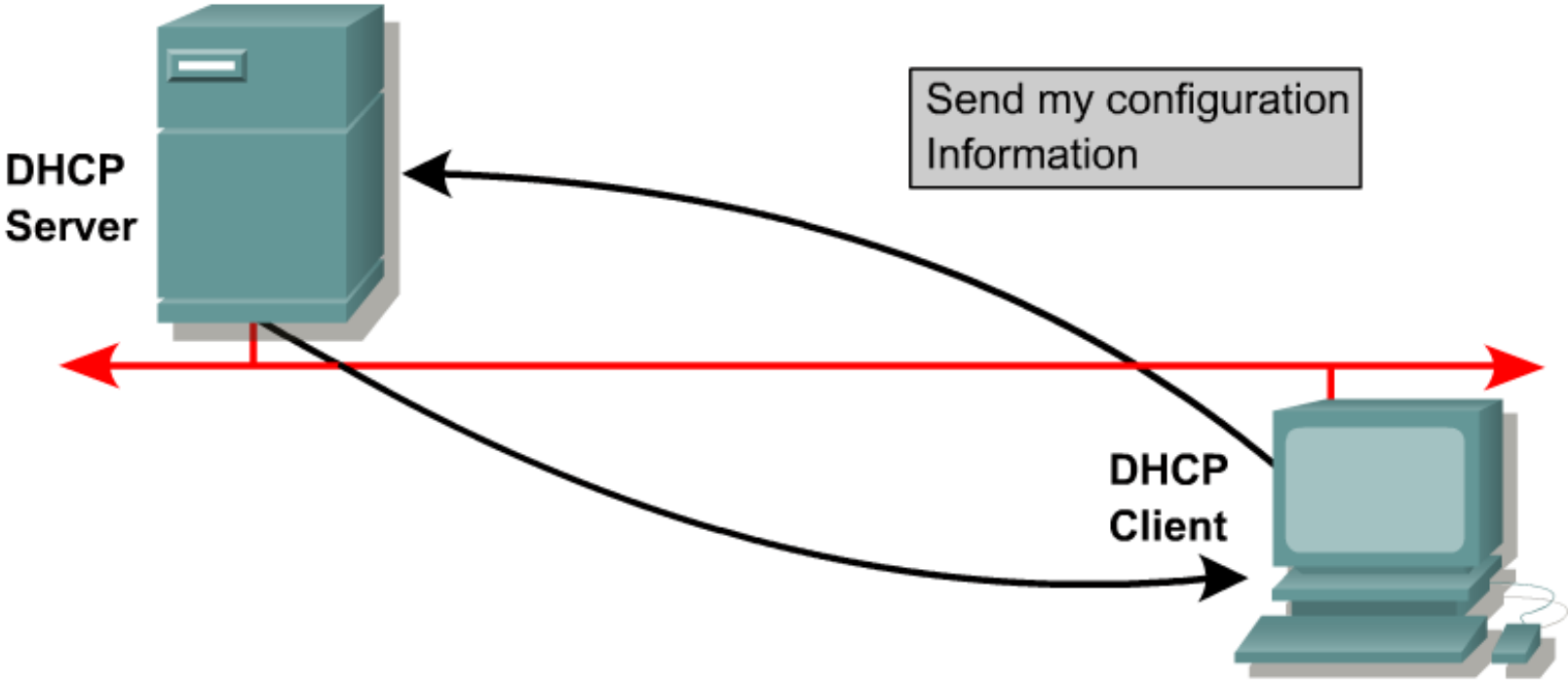
BOOTP and DHCP differences

BOOTP	DHCP
Static Mappings	Dynamic Mappings
Permanent assignment	Lease
Only supports four configuration parameters	Supports over 30 configuration parameters

There are two primary differences between DHCP and BOOTP:

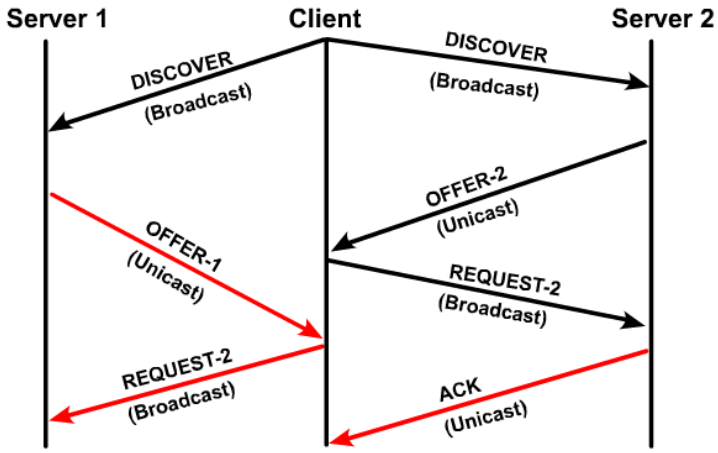
- DHCP defines mechanisms through which clients can be assigned an IP address for a finite lease period.
  - This lease period allows for reassignment of the IP address to another client later, or for the client to get another assignment, if the client moves to another subnet.
  - Clients may also renew leases and keep the same IP address.
- DHCP provides the mechanism for a client to gather other IP configuration parameters, such as WINS and domain name.

Major DHCP features

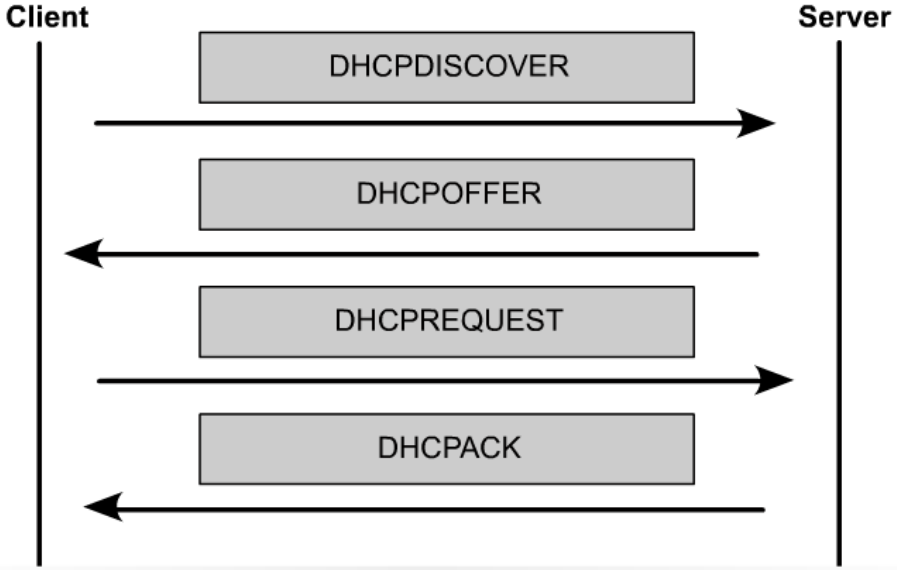


Here is Your Configuration:
- IP Address: 192.204.18.7
- Subnet Mask: 255.255.255.0
- Default Routers: 192.204.18.1, 192.204.18.3
- DNS Servers: 192.204.18.8, 192.204.18.9
- Lease Time: 5 days

DHCP Operation



- DHCP client broadcasts DHCPDISCOVER packet on local subnet
- DHCP servers send OFFER packet with lease information
- DHCP client selects lease and broadcasts DHCPREQUEST packet
- Selected DHCP server sends DHCP ACK packet



DHCP messages in the order they are transmitted

Configuring DHCP


```
Router(config)#ip dhcp pool pool-name1
```

Specify the DHCP pool

```
Router(dhcp-config)#network ip-address mask
```

Specify the range of addresses in the pool

- Creates an IP DHCP pool, and gives it a name
- Multiple DHCP pools can be created on one server
- Specify the IP range of addresses using an IP network address and mask

- Note: The network statement enables DHCP on any router interfaces belonging to that network.
  - The router will act as a DHCP server on that interface.
  - It is also the pool of addresses that the DHCP server will use.

Configuring DHCP


```
Router(config)#ip dhcp excluded-address ip-address [end-ip-address]
```

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

- The **`ip dhcp excluded-address`** command configures the router to exclude an individual address or range of addresses when assigning addresses to clients.
- Other IP configuration values such as the default gateway can be set from the DHCP configuration mode.
- The DHCP service is enabled by default on versions of Cisco IOS that support it. To disable the service, use the **`no service dhcp`** command.
- Use the **`service dhcp`** global configuration command to re-enable the DHCP server process.

Configuring DHCP

Command	Description
network *network-number* [*mask* | *prefix-length*]	Specifies the subnet network number and mask of the DHCP address pool. The prefix length specifies the number of bits that compromise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
default-router *address* [*address2...address8*]	Specifies the IP address of the default gateway for a DHCP client. Although one address is required, up to eight addresses can be specified in one command line.
dns-server *address* [*address2...address8*]	Specifies the IP address of a DNS server that is available to a DHCP client. Although one address is required, up to eight addresses can be specified in one command line.
netbios-name-server *address* [*address2...address8*]	Specifies the NetBios WINS server that is available to a Microsoft DHCP client. Although one address is required, up to eight addresses can be specified in one command line.
domain-name *name*	Specifies the domain name for the client.
lease {*days* [*hours*] [*minutes*] | **infinite**}	Specifies the duration of the lease. The default is a one-day lease.

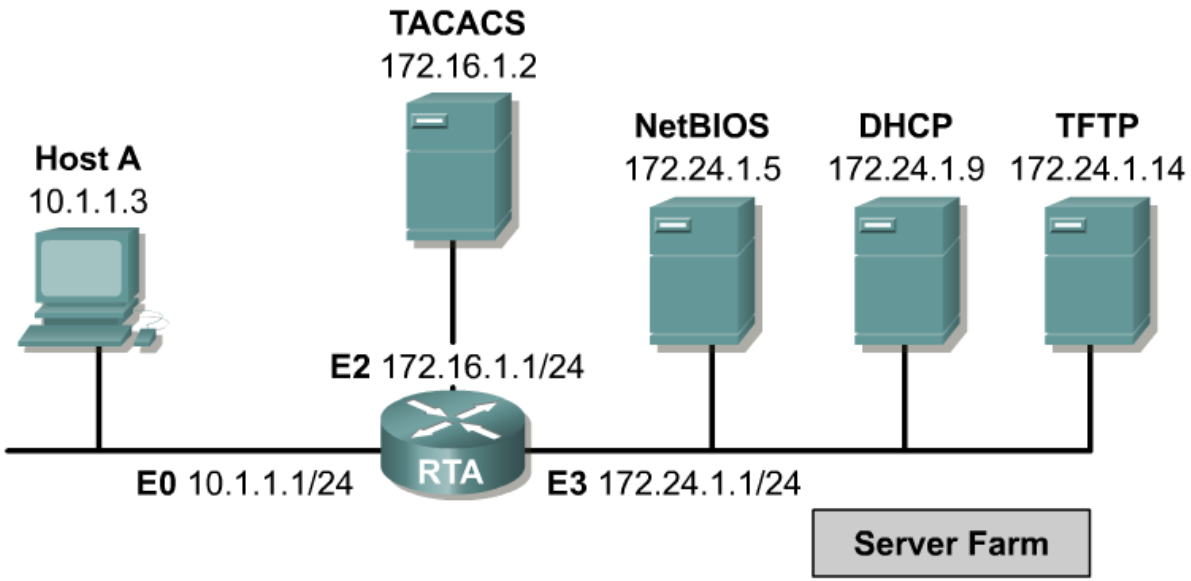
- DHCP options

Verifying and Troubleshooting DHCP


```
Router#show ip dhcp binding
IP address      Hardware address    Lease expiration        Type
172.16.12.11    0100.10a4.97f4.6d   Mar 02 1993 12:38 AM    Automatic
Router#
```

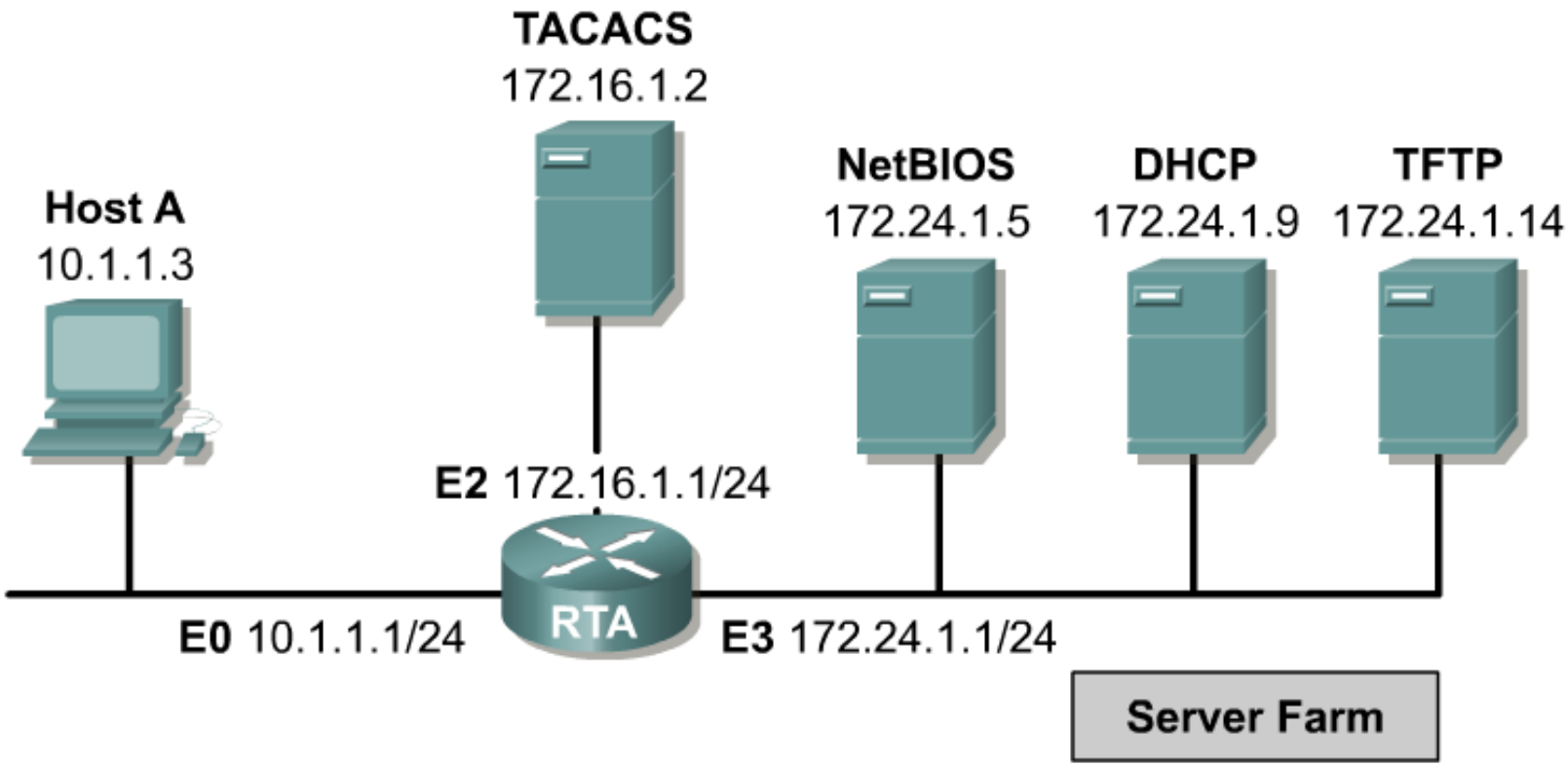
```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD:checking for expired leases.
00:22:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d
00:22:49: DHCPD:retured 172.16.13.11 to address pool remote.
00:22:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a497f4.6d.
```

DHCP Relay



- DHCP clients use IP broadcasts to find the DHCP server on the segment.
- What happens when the server and the client are not on the same segment and are separated by a router?
  - Routers do not forward these broadcasts.
- When possible, administrators should use the **`ip helper-address`** command to relay broadcast requests for these key UDP services.

Using helper addresses



Routers do not forward broadcasts natively, but with the use of the **`ip helper-address`** command, broadcasts can be forwarded by the router to a specific server on another subnet.

Configuring IP helper addresses

By default, the **ip helper-address** command forwards the eight UDPs services.

Default Forwarded UDP Services

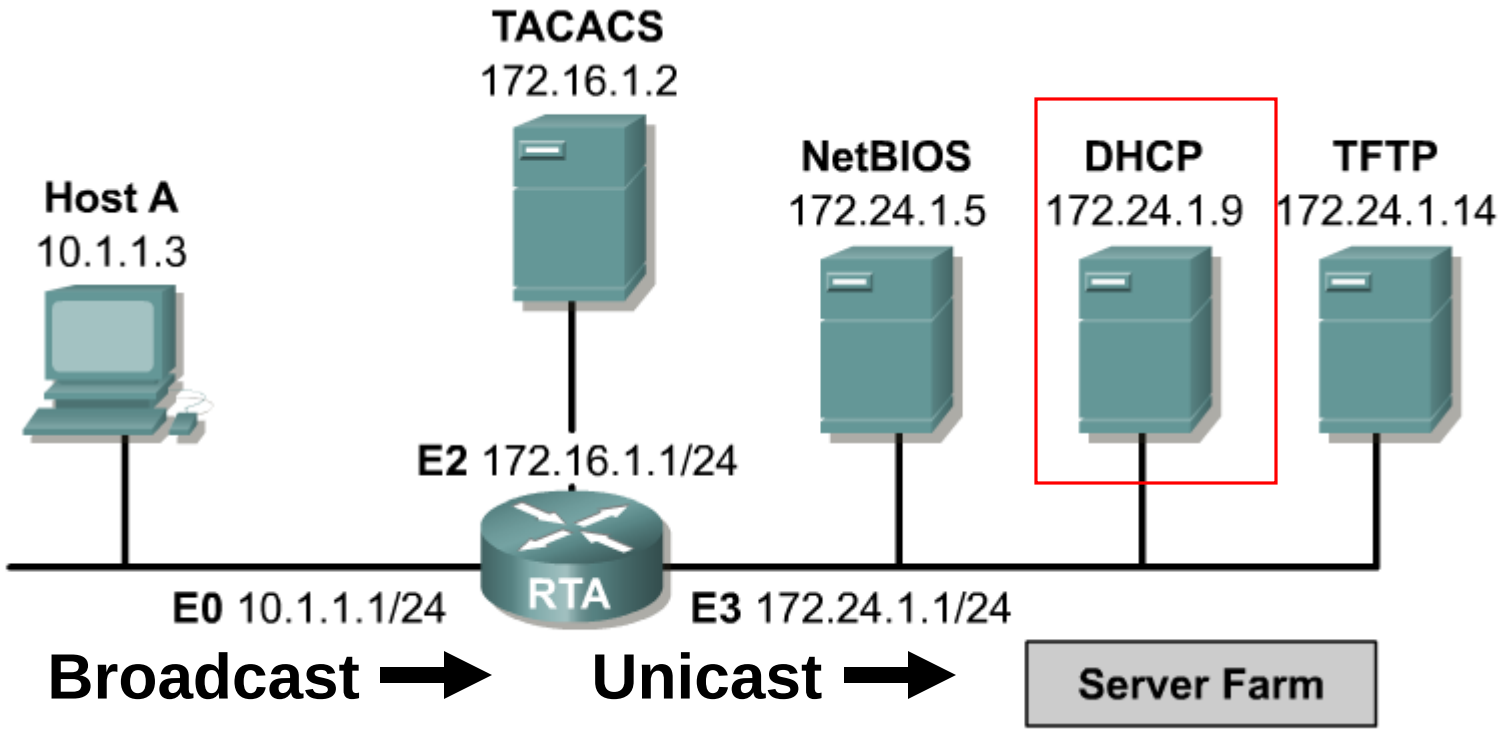
Service	Port
Time	37
TACACS	49
DNS	53
BOOTP/DHCP server	67
BOOTP/DHCP client	68
TFTP	69
NetBIOS name service	137
NetBIOS datagram service	138

Default Forwarded UDP Services

RTA

```
RTA(config-if)#ip helper-address 192.168.1.254
RTA(config-if)#exit
RTA(config)#ip forward-protocol udp 517
RTA(config)#no ip forward-protocol udp 37
RTA(config)#no ip forward-protocol udp 49
RTA(config)#no ip forward-protocol udp 137
RTA(config)#no ip forward=protocol udp 138
```

Configuring IP helper addresses



To configure RTA e0, the interface that receives the Host A broadcasts, to relay DHCP broadcasts as a unicast to the DHCP server, use the following commands:

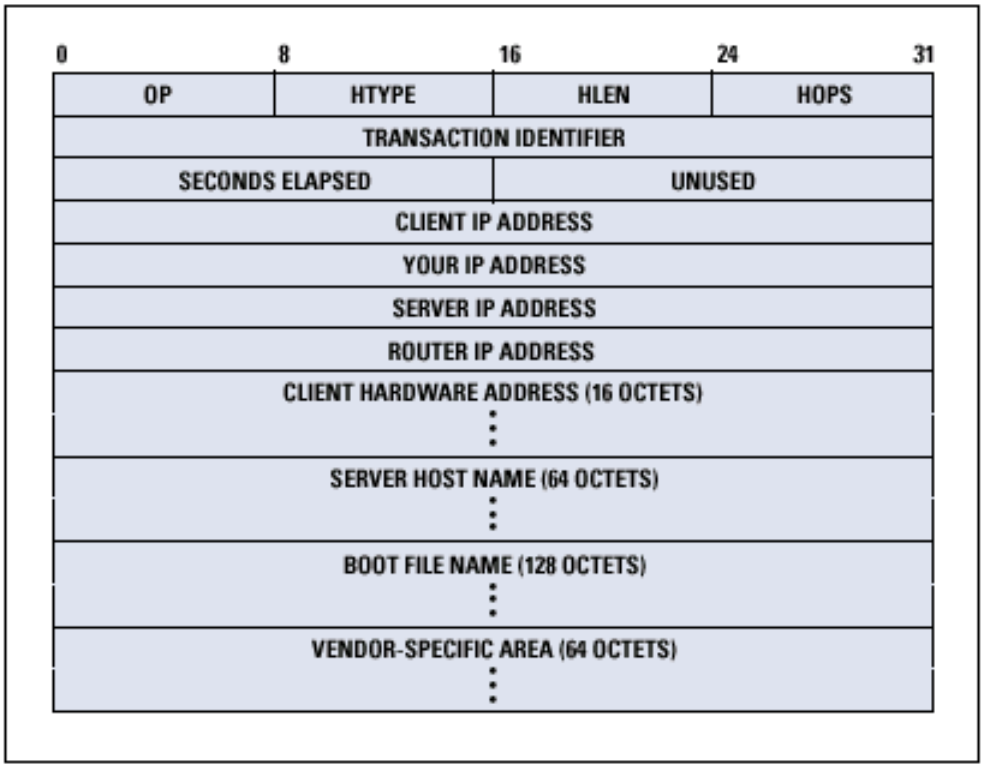
```
RTA(config)#interface e0
RTA(config-if)#ip helper-address 172.24.1.9
```

Role of DHCP/BootP Relay Agent

- Routers, by default, will not forward broadcast packets.
- Since DHCP client messages use the destination IP address of 255.255.255.255 (all Nets Broadcast), DHCP clients will not be able to send requests to a DHCP server on a different subnet unless the DHCP/BootP Relay Agent is configured on the router.
- The DHCP/BootP Relay Agent will forward DHCP requests on behalf of a DHCP client to the DHCP server.
- The DHCP/BootP Relay Agent will append its own IP address to the source IP address of the DHCP frames going to the DHCP server.
- This allows the DHCP server to respond via unicast to the DHCP/BootP Relay Agent.
- The DHCP/BootP Relay Agent will also populate the Gateway IP address field with the IP address of the interface on which the DHCP message is received from the client.
- The DHCP server uses the Gateway IP address field to determine the subnet from which the DHCPDISCOVER, DHCPREQUEST, or DHCPINFORM message originates.
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a00800f0804.shtml#roledhcpbootprelay

Role of DHCP/BootP Relay Agent

DHCP Packet



Ch. 1 – Scaling IP Addresses
NAT/PAT and DHCP

Cabrillo College

CIS 83 (CCNA 4)

Fall 2006

Rick Graziani

Cabrillo College